December 2019

Combining Detected Motion with Multiple Facial Images for Biometric Authentication on an Electronic Device

N/A

Combining Detected Motion with Multiple Facial Images for Biometric Authentication on an Electronic Device

Abstract:

This publication describes techniques for combining detected motion with multiple facial images for biometric authentication on an electronic device. The motion is detected by one or more motion sensors on the electronic device. The motion may be indicative of a gesture made by the user of the electronic device, for example, a twist of the device in the user's hand. Motion information is analyzed to determine a user's intent to access the device. Responsive to determining a user's intent to access the device, multiple images of the user's face are captured by a front-facing RGB camera to build a composite image of the person who is attempting to access the device. The images are analyzed, along with the motion information, to provide biometric authentication for the device.

Keywords:

Authenticate, intent, gesture, twist, electronic device, smartphone, image, frame, video, twist, motion sensors, gyroscope, accelerometer, camera, RGB camera, front-facing, facial recognition, biometric authentication

Background:

Personal identification and authentication on an electronic device (*e.g.*, smartphone) can be performed utilizing multiple cameras (*e.g.*, red, green, and blue (RGB) camera, infrared (IR) camera, depth-sensing camera, etc.) and/or sensors (*e.g.*, fingerprint, biometric security, etc.) embedded in the electronic device. For example, a user of the electronic device may utilize a facial recognition technology implemented on the electronic device in order to unlock or otherwise access the electronic device.

In some embodiments, an electronic device may utilize anti-spoofing techniques to get both two-dimensional (2D) and three-dimensional (3D) information of a user's face. However, these anti-spoofing measures require special hardware (*e.g.*, dot projectors, infrared cameras, etc.), require space on a bezel of the electronic device, and/or may not be available for use on the electronic device.

Due to the cost and availability of hardware, in aspects, facial recognition may be performed with a standard front-facing RGB camera. However, using a simple RGB image of a face from a single RGB camera for biometric authentication can be easily spoofed – an RGB camera does not capture depth information to ensure the image is not of a photograph of a face instead of an actual face.

Therefore, it is desirable to combine detected motion with multiple facial images from a single RGB camera to provide biometric authentication on an electronic device.

Description:

This publication describes techniques for combining detected motion with multiple facial images for biometric authentication on an electronic device. The image capture may be performed using standard RGB camera technology to enable broad, cost-effective adoption. The veracity of the image capture may be confirmed by motion sensors (*e.g.,* gyroscope, accelerometers, etc.) on the electronic device to determine that the electronic device is moving to prevent potential RGB image spoofing with a video or photograph of a face. The electronic device may recognize a gesture, such as a twist of the electronic device, as the indication from the user that the user wants to perform facial authentication and automatically perform the facial recognition.

Figure 1 illustrates an example of this system in an electronic device that supports a multiple facial images user authentication application using a standard front-facing RGB camera.

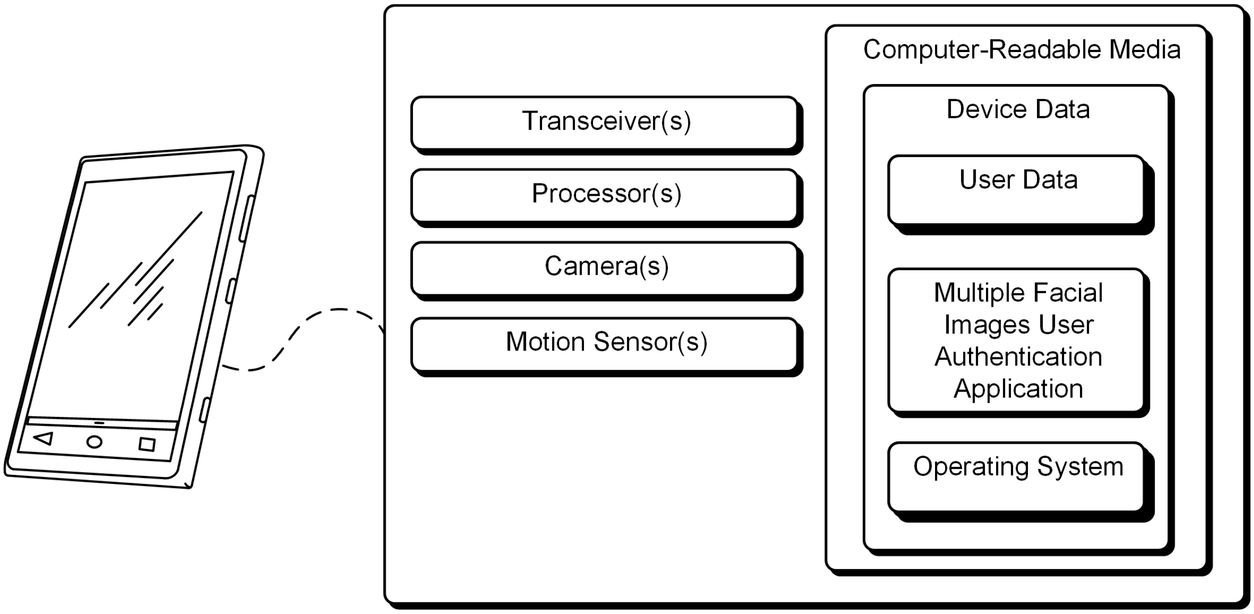

Figure 1

As illustrated, the electronic device is a smartphone. However, other electronic devices (*e.g.*, a tablet, a laptop computer, a wearable device, or the like) can also support the multiple facial images user authentication application described in this publication. The electronic device includes a processor(s), transceivers (*e.g.* 4G LTE, 5G NR) for transmitting data to and receiving data from an access point of a wireless network, one or more cameras (*e.g.*, RGB camera), and one or more motion sensors The electronic device also includes a computer-readable medium (CRM). CRM includes device data. The device data includes user data, multimedia data, applications including a multiple facial images user authentication application (herein "facial authentication application"), and/or an operating system of the computing device, which are executable by the processor(s) to enable analyzing multiple images for authentication. While the facial authentication application could be stored within the CRM, other implementations can include any combination of firmware, hardware, and/or software.

The device data includes executable instructions of a facial authentication application that can be executed by the processor(s). The facial authentication application represents functionality that recognizes a gesture (*e.g.*, a small twist/shake of an electronic device) from a user as indicating an intent to access the electronic device, captures images of a face from multiple angles, analyzes the images, compares motion information from one or more motion sensors with the images to confirm motion of the electronic device, and transmits data regarding user authentication or user rejection to one or more applications on the electronic device. Additionally, the facial authentication application represents functionality that prompts a user to make the gesture (*e.g.*, a small twist/shake) if the user intent is not recognized.

Figure 2, below, illustrates an electronic device that detects a twist or shake of the electronic device, which is recognized as a gesture to perform authentication.

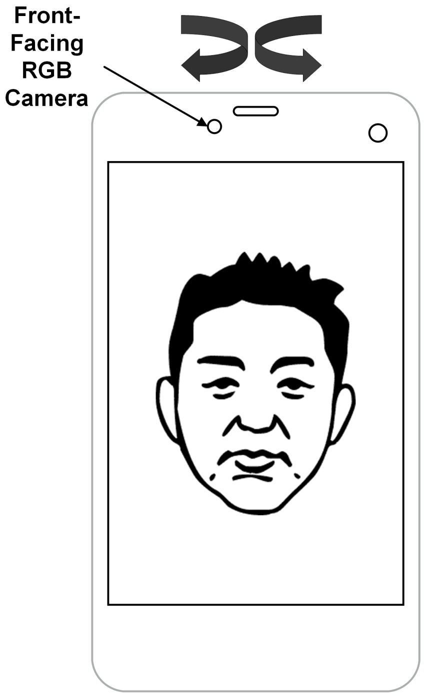

Figure 2

In the use case illustrated in Figure 2, Henry's smartphone is in a locked state, and Henry picks up his smartphone to use it. A facial authentication application on the smartphone first determines if Henry intends to unlock the smartphone, and upon making such a determination, then performs an authentication procedure. To determine Henry's intent, a facial authentication application on the smartphone determines if Henry has made a gesture or otherwise provided an expected input to the smartphone (*e.g.*, a small twist of the smartphone, a shake of the smartphone). If the facial authentication application does not detect the expected gesture, the smartphone may prompt Henry to make the gesture to access the smartphone.

In response to recognizing the gesture, the facial authentication application uses the front-facing RGB camera to capture multiple images of Henry's face and the background at different angles to build a composite image of who is trying to access the smartphone. Multiple images captured with the RGB camera are difficult to spoof with a video in front of the RGB camera because an unauthorized user who is trying to spoof the electronic device would have to match the tilt of a video device with the twist of the electronic device. Image processing on the electronic device can analyze a face in a foreground image and a background of an image to build a composite image with depth information. One or more motion sensors on the phone (*e.g.*, gyroscopes, accelerometers, etc.) can sense how much the electronic device had tilted or moved relative to when image capture began. The facial authentication application compares sensor data with the images to detect spoofing. Based upon the confidence of the images and sensor data, Henry may be authenticated (*e.g.*, to access the smartphone, to access an application on the smartphone, etc.) or may have access rejected.

Further to the above descriptions, a user may be provided with controls allowing the user to make an election as to both if and when systems, applications, and/or features described herein may enable collection of user information (*e.g.*, photographs of a user, information about a user's social network, social actions, social activities, profession, a user's preferences, a user's current location), and if the user is sent content and/or communications from a server. In addition, certain data may be treated in one or more ways before it is stored and/or used so that personally identifiable information is removed. For example, a user's identity may be treated so that no personally identifiable information can be determined for the user. In another example, a user's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level) so that a particular location of a user cannot be determined. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user.

References:

[1] Patent Publication: US20180239955A1. Liveness detection. Priority Date: August 10, 2015.

[2] Patent Publication: US20130063611A1. Initializing Camera Subsystem for Face Detection Based on Sensor Inputs. Priority Date: September 9, 2011.